Malformed X.509 certificates

What's it about?
Certificate authorities sometimes disregard specifications and issue certificates that lead to apparent errors and potential vulnerabilities. On a large-scale, this project aims to identify certificates that are violating basic requirements. By detecting misissued certificates and rogue CAs, you contribute to strengthen the global chains of trust.

Goals:
- Investigate trust relationships between certificates
- Uncover practices that puts the certificate security at risk
- Identify frequent configuration problems

Interests:
- Trust and Certificates
- Large-scale analysis

Impact:
- Draws a picture/statistics of global certificate misuse
- Points out structural flaws in PKI systems

Contact: peter.teufl@iaik.tugraz.at